THE LONG ARM OF THE LAW

American Bribery and Trade Sanctions Prosecutions in a Global Environment

INTRODUCTION

American regulators are rightly feared for the ferocity of the laws they enforce. What companies sometimes fail to appreciate, however, is the zeal with which regulators apply those laws to entities with few ostensible ties to the United States.

This paper briefly outlines some of the extraterritorial traps that US regulators can spring on unsuspecting companies. Some of those companies might do regular business in the United States, but (wrongly) consider themselves at low risk of investigation for activities that take place far from American shores; others believe they are well removed from US jurisdiction on any ground, yet still become ensnared.

Whole books have been devoted to the long arm of US law. We will touch on the main points. We focus on two aspects of US law of proven risk in the international sphere: corruption and trade sanctions. We address each in turn.

CORRUPTION

Overview

The United States was the first nation to enact a law criminalizing the bribery of foreign public officials.1 Although other nations have caught up on paper, American regulators remain by far the most zealous in their efforts to investigate and prosecute foreign corruption.

Up until 2004, the US Department of Justice and US Securities and Exchange Commission accounted for 100% of anti-bribery enforcement actions—despite the fact that other nations had by then had foreign anti-bribery laws on their books for several years.2 As of the end of 2010, in the face of significantly more aggressive stances from some European regulators, the US still accounted for 70% of all formal anti-bribery charges (the UK was a distant second, with 4%).3 And those statistics say nothing about the number and scope of time-consuming investigations that US regulators initiate against companies.

Note, further, that all but two of the top ten anti-bribery fines in the US have been leveled against non-US companies; that the smallest of these fines amounted to $70 million (the largest to date, paid by

---

1 The Foreign Corrupt Practices Act, 15 USC §§ 78dd-1 and 2.
Siemens, was for about $850 million); and that all of these top ten fines were imposed in 2009, 2010, and 2011. This is not, in short, an insubstantial, remote, or fading risk.

**History**

The history of anti-bribery legislation in the US is interesting in its own right. The impetus for what ultimately became known as the Foreign Corrupt Practices Act (FCPA) came originally from the aftermath of the Watergate scandal. Although a byword for purely political misdeeds, the Watergate saga spurred a series of wide-ranging investigations into corporate (mis)behavior.

The US Securities and Exchange Commission asked thousands of listed companies to provide information about their campaign contributions and other attempts to influence domestic politics. Under the Federal Election Campaign Act of 1971, as amended in 1974, individuals and corporations needed to disclose their political contributions, and were limited in the amounts they could donate.

Two consequences followed. First, the SEC – having issued all these subpoenas and requests for information – quickly realized that it lacked the manpower to cope with the document deluge that would follow. The SEC therefore began an amnesty program: any company that retained an outside law firm to conduct an independent inquiry and that reported the results of that inquiry to the SEC, would escape sanction.

About 400 companies made use of the amnesty program (thereby providing an enormous boost to their law firms). Thus was born the so-called internal investigation; it is a mode of doing regulatory business that prevails to this day. Even when the SEC or DOJ initiates an investigation (as opposed to a company’s self-reporting a potential problem), US regulators will expect the company in question to retain lawyers to do much of the work. This has proven extremely time-consuming and expensive for those targeted companies.

The second consequence of the SEC’s subpoenas in the mid-1970s stemmed from what the law firms actually found in the course of their internal investigations. Rather than discovering widespread campaign contribution fraud – which was what the SEC had expected to find – the internal investigations unearthed massive slush funds for the express purpose of bribing foreign officials.

At the time this was perfectly legal. But it was distasteful in a cultural climate formed after a national scandal revolving around the misuse of power and the diversion of resources for personal and political gain.

---

6 2 USC § 431 et seq.
7 “Specter blasts fine-only approach to FCPA enforcement,” Corporate Counsel, December 1, 2010.
9 SEC Report at 56.
The findings of the investigations thus prompted Congress to consider legislation prohibiting bribery of foreign officials. The Ford Administration opposed the legislation, preferring voluntary disclosures to criminal sanctions.  

But President Ford lost the election of 1976 to Jimmy Carter. Carter’s campaign had made much of the ethical improprieties that had plagued the body politic earlier in the decade. The idea of a law that punished Americans for unethical behavior wherever that behavior occurred aligned with the broader message of the Administration. And so the FCPA became law in 1977.

The OECD Convention

It would be more than two decades before any other nation had a comparable law to prohibit bribery of foreign officials. It would have been longer still if the United States had not brought to bear considerable pressure on them to do so.

That pressure was the result of a concerted effort by US businesses to lobby the US government: American companies (rightly) considered themselves at a competitive disadvantage. Whereas a European company could blithely bribe a Minister or a prince to win a contract – and then claim that bribe as a tax deduction – its US counterpart had to play the Boy Scout (or at least had to be discreet about committing what for it was a crime).

After years of pushing, the Organization for Economic Cooperation and Development enacted the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions of December 17, 1997. The Convention called on Member States – several dozen of the world’s richest and most advanced nations – to adopt legislation criminalizing bribery of foreign officials.

They have since done so, with varying degrees of enthusiasm and effectiveness. But United States authorities remain by far the most aggressive and enthusiastic regulators and prosecutors of international corruption.

Substantive Provisions

The FCPA makes it a criminal offense to provide payments or “anything of value” to a foreign public official in furtherance of an attempt to “obtain or retain business.”

The FCPA defines a “foreign public official” broadly:

---

10 House Report at 19.
14 37 I.L.M. 1.
15 15 USC §§ 78dd-1(a); 78dd-2(a); 78dd-3(a).
[A]ny officer or employee of a foreign government or any department, agency, or instrumentality thereof, or of a public international organization, or any person acting in an official capacity for or on behalf of any such government or department, agency, or instrumentality, or for or on behalf of any such public international organization.\footnote{16}{15 USC §§ 78dd-1(f); 78dd-2(h)(2)(A).}

Past prosecutions have been mounted on the basis of payments to officers in state-run corporations,\footnote{17}{A federal court in California recently rejected a defendant’s challenge to the standard interpretation of the FCPA that officers of state-owned companies qualified as “foreign officials” within the meaning of the FCPA. See United States v. Enrique (“Lindsey Manufacturing”), 2:10-Cr-01031-AHM (C. D. Cal. April 20, 2011).} payments to members of royal families in monarchies,\footnote{18}{See, e.g., “BAE Systems PLC Pleads Guilty and Ordered to Pay $400 Million Criminal Fine,” http://www.justice.gov/opa/pr/2010/March/10-crm-209.html (March 1, 2010).} and remuneration of one kind or another to doctors in countries with state-run health care systems.\footnote{19}{See, e.g., “Johnson & Johnson Agrees to Pay $21.4 Million Criminal Penalty to Resolve Foreign Corrupt Practices Act and Oil for Food Investigations,” http://www.justice.gov/opap/2011/April/11 crm-446.html (April 8, 2011).}


The FCPA permits one exemption from and two affirmative defenses to prosecution. The exemption is for small payments to facilitate routine, non-discretionary governmental tasks – processing visas, keeping the lights on.\footnote{23}{See, e.g., Arthur F. Mathews, Defending SEC and DOJ FCPA Investigations and Conducting Related Corporate Internal Investigations: The Triton Energy/Indonesia SEC Consent Decree Settlements, 18 NW J. Int. L. & Bus. 303 at 15 (1998).} The DOJ, however, has frowned on payments that it does not dispute are facilitation payments but that it nonetheless views as excessive. Even payments as low as $1,000 have been questioned.\footnote{24}{See, e.g., United States v. Kozeny, 582 F. Supp.2d 535 (S.D.N.Y. 2008).}

The first affirmative defense to prosecution is for payments made in countries where the written law expressly permits such payments.\footnote{25}{15 USC §§ 78dd-1(c); 78dd-2(c); 78dd-3(c).} With the possible exception of China (where one of the authors once contended to prosecutors that a statute criminalizing bribery over a certain sum implicitly meant that bribes to officials under that sum were legal),\footnote{26}{Criminal Code of the People’s Republic of China, Arts. 383, 385, 386, 389, 393 (Revised June 29, 2006).} there is no country associated with an FCPA prosecution that has such a law on its books. US courts likewise have yet to sustain a defense based on this claim.\footnote{27}{See, e.g., United States v. Kozeny, 582 F. Supp.2d 535 (S.D.N.Y. 2008).}

The second affirmative defense is for reasonable and \textit{bona fide} expenditures relating to the demonstration of a product or service or to the performance of a contract.\footnote{28}{15 USC §§ 78dd-1(c); 78dd-2(c); 78dd-3(c).} For example, it would be
permissible to pay the expenses and accommodation of foreign officials to visit a manufacturing plant in Turin. If the foreign officials were also treated to two weeks in a villa in Tuscany and a yacht trip through the Adriatic, it would raise eyebrows.

Companies should also beware of so-called “local content” provisions in various jurisdictions: ostensibly these are regulations to ensure that a minimum portion of a project’s sub-contracts and corollary work is performed by a local entity. In fact, these provisions sometimes disguise a situation where the only licensed or available sub-contractor is in fact a company itself owned by, or with close ties to, a foreign official. Companies therefore must undertake rigorous due diligence of such contractors and collaborators, even when they are employing them in order to satisfy the requirements of local laws.

**Jurisdiction**

A non-US company would be forgiven for wondering what any of this has to do with it. Surely the provisions of a US law are a matter only for US companies?

Unfortunately not. This is what makes the FCPA – and indeed US regulators in general – so dangerous.

The basic jurisdictional provisions of the FCPA do indeed look reasonably calculated to deal only with US entities. On its face the FCPA applies either to “issuers”\(^{29}\) or to “domestic concerns.”\(^{30}\) Persons or entities that are neither “issuers” nor “domestic concerns” can still be liable for FCPA violations, however, for actions they take while on United States territory\(^ {31}\) (on which more below).

An “issuer” is a company that has a reporting obligation to the SEC.\(^ {32}\) This includes foreign companies trading Level II or Level III (but not Level I\(^ {33}\)) American Depository Receipts on a US exchange.\(^ {34}\) A “domestic concern” is a US-incorporated company or partnership, or a US individual.\(^ {35}\)

So far, so normal. The problem is two-fold: first, American regulators have hinted on more than one occasion that they view the FCPA’s territorial nexus provision – the provision conferring jurisdiction for acts taken in the United States\(^ {36}\) – to be extremely elastic. Thus, the DOJ has targeted a French company making illicit payments to Nigerian officials from a Dutch bank account to a Swiss bank account.\(^ {37}\) Because the funds transferred was in US dollars, the DOJ alleged that these funds passed

\(^{29}\) 15 USC § 78dd-1(a).

\(^{30}\) 15 USC § 78dd-2(a).

\(^{31}\) 15 USC § 78dd-3.

\(^{32}\) 15 USC § 78m(b)(2).

\(^{33}\) A Level I American Depository Receipt permits a company listed on a foreign exchange to trade its shares in the United States. It does not obligate the company, however, to file periodic reports with the SEC, or to report its revenue in conformity with US Generally Accepted Accounting Principles. Level II and III ADRs require a foreign company to file certain reports with the SEC, thus qualifying them as “Issuers” under the FCPA definition.

\(^{34}\) 15 USC § 78l(f)(1)(A).

\(^{35}\) 15 USC § 78dd-2(h).

\(^{36}\) See note 31 above.

through correspondent banks in the United States. Similarly, the SEC’s complaint against Siemens alleged that certain improper payments passed through US bank accounts.

To be sure, both the DOJ and SEC had other “hooks” in both cases on which to hang their assertions of jurisdiction. But the references to correspondent bank accounts are ominous because it is very easy indeed to become involved in a correspondent bank transaction: it happens any time a large amount of US currency is at issue.

If a Spanish company, for example, wishes to pay a Swiss counterparty in US dollars, the transaction will likely involve a US correspondent bank. The company’s Spanish bank is unlikely to have enough American currency on hand simply to effectuate the transaction. So the Spanish bank will wire Euros to its correspondent in the US. The US correspondent will then wire the equivalent and desired dollar amount to the US correspondent of the Swiss destination bank, which will then remit the amount to Switzerland.

Even the most straightforward transactions, therefore, can potentially subject non-US companies to the jurisdiction of the United States.

The second problem for companies ostensibly outside the remit of the FCPA is that both the SEC and DOJ have used other jurisdictional tools at their disposal to craft suits against non-US companies for FCPA violations.

Hence, defense contractor BAE Systems paid $400 million in 2010 after a guilty plea in connection with worldwide bribes to foreign officials. BAE is not a “domestic concern” within the meaning of the FCPA – it is a British company. Nor did BAE trade shares on an American exchange such that it qualified as an “issuer” for FCPA purposes.

Rather than charge BAE with FCPA violations, therefore, the DOJ accused BAE of having lied to US officials about the adequacy of its anti-bribery controls. It is a crime to make a false statement to a US government official – even if one is not under oath. The DOJ appended a letter from November 2000 from BAE’s Chief Executive to then-Secretary of Defense William Cohen to its Criminal

---

38 Id. at ¶ 22.
41 United States of America v. BAE Systems plc (D. D.C. February 5, 2010). Technically, the DOJ filed a one-count criminal information against BAE alleging conspiracy, inter alia, to make false statements. The conspiracy charge was necessary to preserve the allegation of false statements from a statute of limitations defense. The statute of limitations for a conspiracy runs from the date of the last overt act in furtherance thereof. More on conspiracy below.
42 18 USC § 1001.
Information. The letter described BAE’s commitment to the “highest ethical standards in the conduct of its business throughout the world.”

A company doing business in the United States may therefore remain technically outside the scope of FCPA jurisdiction for activity unrelated to its US operations that it undertakes outside the United States. But companies in such a posture should beware that US regulators may find other ways to assert jurisdiction over their foreign activity. And even if the DOJ were to conclude that no crime was committed, its investigation prior to that conclusion would doubtless be onerous and intrusive.

Note, in similar vein, that US authorities have not hesitated to assert jurisdiction over individuals for FCPA violations even if they are merely passing through the United States. The case in point is that of Christian Sapsizian. Sapsizian was a French citizen accused of having bribed Costa Rican officials on behalf of the French company for which he worked (Alcatel).

Sapsizian was not working in the United States, was not a permanent resident of the United States, and had made no US-based plans to effect Alcatel’s bribery scheme. His mistake was to fly from Panama to Paris on a plane that stopped to refuel in Miami. It was there that he was arrested.

What, then, if a company has no presence in the United States, does no business there, sends no employees there, and avoids large dollar-denominated transactions? Even in that (unlikely) scenario, US regulators have advanced theories that might confer jurisdiction over any such company’s corrupt activities. They have done so by alleging a conspiracy.

A brief description of the Anglo-American concept of criminal conspiracy is in order for readers who do not hail from common law jurisdictions. Conspiracy is effectively a thought crime: it is illegal to contemplate doing something illegal in future, even if you have yet to do it. This might sound strange, but it forms the basis for a great deal of US prosecutorial activity, not least against would-be terrorists.

In order to prove a conspiracy, the government must show that two or more parties agreed to embark upon a criminal enterprise, and that at least one party engaged upon one or more actions in furtherance of that conspiracy.

43 A Criminal Information is a charging document under US law. It differs from an Indictment inasmuch as a prosecutor can file the former, but not the latter, without a Grand Jury.
44 United States of America v. BAE Systems plc (D. D.C. February 5, 2010), Ex. A.
45 Alcatel merged with US company Lucent in December 2006. The activities of which Sapsizian had been accused took place before the merger. US authorities took the view that they had jurisdiction over the merged firm for Alcatel’s pre-merger activities. Alcatel-Lucent settled the FCPA case for $137 million in December 2010. See “SEC Charges Alcatel-Lucent for FCPA Violations,” SEC Release No. 2010-258 (December 27, 2010).
48 18 USC § 371.
The actions themselves – “overt acts” in the parlance of American criminal law – need not be criminal at all: they can be as innocent as a phone call.49 For example, let us suppose that you (the reader) and one of the authors agreed it would be a good idea to steal the Mona Lisa. If one of us then called the Louvre to ask what time it closed, that phone call would qualify as an overt act for the purpose of proving our conspiracy.

The significance for the FCPA is that US authorities can charge non-US entities with no ties whatsoever to the United States with conspiracy to violate the FCPA if they are engaged in some kind of joint venture with other companies that do have a nexus to the United States. Because US prosecutors only need to show one overt act in furtherance of a conspiracy, and because one – and only one – of the co-conspirators need engage in such an act, prosecutors can allege jurisdiction over the non-US entities with no ties to the US by virtue of the act(s) committed by any other entities in the joint venture.

This is exactly what the DOJ did in April 2011 with JGC. JGC is a Japanese engineering corporation. It was part of a multinational consortium tasked with building a liquefied natural gas plant off the coast of Nigeria. One of the other members of the consortium was Halliburton subsidiary Kellogg Brown & Root. After the DOJ successfully forced a guilty plea and $400 million fine from Halliburton,50 it turned to JGC.

The Criminal Information against JGC accuses the Japanese company of conspiracy to violate the FCPA.51 The conspiracy arises by virtue of JGC’s interaction with Halliburton and others in the consortium, although JGC concededly had no links to the United States.52 JGC paid a fine of $218.8 million.53

The message is clear: if there is any way that US authorities can assert jurisdiction over a non-US company, they will. This is especially so if the company’s home jurisdiction declines to act.54

It remains to be seen what effects the UK’s new Bribery Act (in force as of July 1, 2011) will have on the global anti-corruption landscape. There are certain inconsistencies between the Bribery Act and the FCPA, as well as between the plain language of the Bribery Act and the guidance on the Act that the Government published on March 31, 2011.55

There is uncertainty in particular about how broadly the UK will cast its own jurisdictional net: the Bribery Act purports to grant jurisdiction to UK authorities to over any entity that “carries on a

49 See, e.g., United States v. Naranjo, 14 F.3d 145 (2d Cir. 1994).
52 Id. at ¶¶ 16-20.
54 This was the case with BAE Systems. Authorities in the UK had dropped the part of their investigation pertaining to alleged bribes in Saudi Arabia. The DOJ took up the investigation as described above.
business, or part of a business, in any part of the United Kingdom."56 The guidance backs away from that aggressive posture,57 but the ultimate regulatory position is unclear.

The Bribery Act on its face is even more stringent than the FCPA. First, it applies to officers in private companies as well as to public officials.58 Companies with extensive UK operations would therefore be well advised to expand whatever anti-bribery procedures they have in place to prohibit any kind of improper payment – not just those that apply to foreign public officials.

Second, unlike the FCPA, the UK Bribery Act contains no exemption for facilitation payments.59

Third, the UK Bribery Act provides that a company whose officers or agents are found to have used bribes to further the company’s business prospects is *automatically* guilty of an offense,60 unless the company can show that it had “adequate procedures” in place to designed to prevent such misconduct.61

Despite a clamor for clarity, the UK Government declined to set forth specific guidance as to exactly what such “adequate procedures” should be. The Government instead set forth six “principles” that it suggested should inform any “adequate” compliance program.62

Unsurprisingly, more than a few company executives have been left scratching their heads over whether the Bribery Act applies to them, and if so what exactly they should do to comply with it. The problem is certainly something of which non-American and non-British companies should remain aware.

**OFAC**

The bulk of this note has focused on the FCPA because of its prominence and its potential for heavy regulatory sanction. A much lesser-known, but almost equally dangerous, regulatory risk lurks in the activities of the Office of Foreign Assets Control in the US Treasury Department.

OFAC has existed in one form or another since prior to the War of 1812.63 Its stated purpose is to regulate the flow of assets to and from the United States to unsavory governments and individuals.64 OFAC does this in two ways: by promulgating regulations to prohibit transactions with specific individuals; and by monitoring and investigating trade sanctions against regimes designated by the President or by the Congress.
SDNs

OFAC maintains prohibitions against doing business with individuals (and some companies) through a list of so-called Specially Designated Nationals (SDNs). The list is publicly available.65 Americans (more below on who is an American for these purposes) cannot do business with anyone on the list.

US banks check every transfer they make against the SDN list. Recall that any substantial dollar transfer anywhere in the world will have to go through a US bank. Many companies without any link to the US will thus find their transfers trapped because they have chosen to do business and to transact in dollars with people on the SDN list. Others find their assets blocked because their names are similar to those of people on the list (this is a particular problem with people from the Middle East).66

Trade Sanctions

The trade sanctions regime is considerably more complicated. Sanctions range from prohibitions on dealing with certain government officials and their close associates (Zimbabwe,67 Belarus68) to near-total embargoes (Cuba69).

The principal sanctions are against Cuba, Iran,70 and North Korea.71 Since North Korea is hardly a fertile source for international commerce, the bulk of activity and controversy centers on Cuba and Iran.

The Cuba embargo prohibits virtually all American involvement in Cuban commerce. This includes non-US subsidiaries of US companies.72 The Iran sanctions similarly prohibit most commerce with Iran. There are exceptions, however, for food and medicine – a loophole that soft drink makers such as Pepsi have exploited to do business there.73 Furthermore, unlike Cuba, non-US subsidiaries of US companies are generally not covered by the sanctions.74

But non-US companies doing business in Iran should not think the story ends for them there. The Iran Sanctions were modified in July 2010.75 The modification imposes sanctions on non-US companies that spend $20 million or more in a 12-month period trading with or investing in Iranian interests in the

66 The SDN List includes, among others, the names of individuals with actual or suspected ties to terrorists organizations in the Middle East. The range of traditional Middle Eastern (Arab) names is somewhat limited, given the tradition of naming boys (and girls) after characters in the Quran. Suspected terrorists therefore share the same name with hundreds, or even thousands, of upstanding and perfectly innocent citizens of Middle Eastern countries.
71 http://www.treasury.gov/resource-center/sanctions/Programs/Pages/nkorea.aspx.
74 See 31 CFR 560.314 (defining “US Person” without including subsidiaries of US entities); compare with 31 CFR 515.329(d) (Cuban Assets Control Regulations).
energy or military sectors. The threat of sanctions persuaded a number of European and Asian energy firms to curtail their activities in Iran.76

Non-US companies accordingly should recognize the growing jurisdictional reach of US economic sanctions. In particular, involving American employees and subsidiaries in decisions pertaining to sanctioned countries will expose them to civil and criminal penalties. Companies therefore should understand who is subject to OFAC’s regulations.

**Jurisdiction**

The sanctions cover all “US Persons.” The definition of who is a US Person, confusingly, varies slightly from one sanctions regime to the next. Generally, a US Person means: i) any US Citizen or permanent resident (Green Card holder), wherever they are in the world; ii) any US-incorporated company or partnership (and any subsidiary thereof for the purpose of the Cuba sanctions but not the Iran sanctions77); iii) any person physically in the United States, even temporarily, irrespective of their citizenship.

So, for example, a US employee of a French company cannot take any action in respect of any transaction involving Iran; a Brazilian executive, in transit at JFK airport and participating in a conference call about Cuban business, would thereby violate the regulations.

**Penalties**

The regulations provide for both civil and criminal penalties. The civil penalties are “strict liability:” they operate whether or not the person knew the relevant facts or law.78 So, again by way of example, if a cigar shop in Paris sold an American citizen a box of Cuban cigars under pretense that the cigars were actually Dominican, the unsuspecting American buyer would still technically have violated the regulations. Although this is a trivial hypothetical, penalties for more serious civil violations can amount to hundreds of thousands of dollars.79 Note that OFAC can assess this penalty for each discrete prohibited transaction. A series of 10 prohibited bank transfers, therefore, can generate a civil penalty of millions of dollars.

---

76 Non-US companies, similarly, should note the remit of the Department of Commerce’s Bureau of Industry and Security. BIS regulations prohibit the re-export of US-origin goods to sanctioned countries. It would be against BIS regulations, for example, to purchase US materials for the purpose or with the intent of exporting them to Cuba – even if the purchaser of the goods itself was a non-US company not subject to the OFAC regulations. See 15 CFR 736.2(b)(6).

77 See Note 75 above.


79 See http://www.treasury.gov/resource-center/Documents/interim_pol_11272007.pdf (increasing maximum civil penalty for civil violations to $250,000).
Criminal penalties apply for “willful” violations of the sanctions regulations. These can involve fines of millions of dollars and jail time of up to 20 years.\textsuperscript{80} Once again, the prospect of conspiracy for violating OFAC regulations – despite not being a US Person – remains a theoretical possibility.

So, if you are a non-American company doing substantial oil and gas business with an Iranian connection, beware: your activity may impede you from access to American markets and finance. If yours is a multinational enterprise dotted with American citizens, Green Card holders, and employees who do business at any time in the United States, be forewarned: their involvement in any decision-making with respect to sanctioned countries and individuals will subject them – and potentially your company – to civil and criminal penalties. And if you transact business in US dollars, know this: any transactions touching on a sanctioned country or a SDN are liable to be frozen in transit through a US correspondent bank.

The risks are legion and the rules complex. Tread with caution.

---

For more information or if you have questions concerning this topic, please contact the Thompson & Knight lawyer with whom you regularly work or one of the lawyers listed below.

**CONTACTS:**

<table>
<thead>
<tr>
<th>Paul H. Cohen</th>
<th>Philip J. Kessler</th>
</tr>
</thead>
<tbody>
<tr>
<td>+1.212.751.3014</td>
<td>+1.212.751.3003</td>
</tr>
<tr>
<td><a href="mailto:Paul.Cohen@tklaw.com">Paul.Cohen@tklaw.com</a></td>
<td><a href="mailto:Philip.Kessler@tklaw.com">Philip.Kessler@tklaw.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Andrew B. Derman</th>
<th>Timothy R. McCormick</th>
</tr>
</thead>
<tbody>
<tr>
<td>+1.214.969.1307</td>
<td>+1.214.969.1103</td>
</tr>
<tr>
<td><a href="mailto:Andrew.Derman@tklaw.com">Andrew.Derman@tklaw.com</a></td>
<td><a href="mailto:Timothy.McCormick@tklaw.com">Timothy.McCormick@tklaw.com</a></td>
</tr>
</tbody>
</table>

---

This white paper is sent for the information of our clients and friends. It is not intended as legal advice or an opinion on specific circumstances and is not intended or written to be used, and may not be used, by any person for the purpose of avoiding penalties that may be imposed under United States federal tax laws.

©2011 Thompson & Knight LLP

---

\textsuperscript{80} http://www.treasury.gov/resource-center/sanctions/Documents/facbk.pdf